UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,326	12/12/2003	Sladjana Petrovic	38898-0059	9081

23577 7590 04/29/2008

RIDOUT & MAYBEE
SUITE 2400
ONE QUEEN STREET EAST
TORONTO, ON M5C3B1
CANADA

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
04/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/733,326	PETROVIC, SLADJANA	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed 12-23-2003.

2. Claims **1 - 34** are pending. Claims **1 - 10, 13, 15 - 17, 21, 23, 25 - 27, 31, 32** have been amended. Claims **1, 13, 23** are independent.

Response to Arguments

3. Applicant's arguments filed 8/31/2007 have been fully considered but are not persuasive. Applicant has raised some good points but the set of referenced prior art addresses these issues.

3.1 Applicant argues the obviousness rejection. (see Remarks Pages 9-11)

Each obviousness combination indicates the claim limitation(s) the combined reference prior art teaches. In addition, a cited passage from the referenced prior art indicates the motivation for the obviousness combination. Each obviousness combination's disclosure is equivalent to the Applicant's claimed limitation(s) for the claimed invention.

Achieved advantage is a valid or desirable motivation for the combination of referenced prior art. The combination of each referenced prior art combination states a motivation for the combination, which translates to an achieved advantage for the combination.

It is not a requirement that the referenced prior art solve the same problem as claimed invention in order to be combinable. There are three criteria for combination:

(1) same file of endeavor (which is session management); (2) motivation for the combination (stated in Office Action); and (3) successful disclosure of claim limitation due to prior art combination. All three criteria are satisfied by the Office Action. (see Williams paragraph [0016], lines 1-4; paragraph [0036], lines 1-2; see Woods paragraph [0047], lines 6-14; paragraph [0057], lines 21-24; see Bachman col. 1, lines 65-67: same field of endeavor: session management)

3.2 Applicant argues that the referenced prior art does not disclose, transmitting session token directly between servers. (see Remarks Pages 11-17)

There is no disclosure for the amended limitation of transmitting said session token directly to the second server. Applicant indicated that paragraph [0038] provides disclosure for this claim limitation. There is no disclosure within paragraph [0038] for the direct transmission of a session token between two servers. (see 112 Rejection)

The Williams prior art discloses the capability to redirect a request from one server to a second server. (see Williams paragraph [0067], lines 12-18: redirection of session token and session information) And, the Williams and Wood combination discloses the capability to transmit a session token at the same time as a redirect request is transmitted between the first and second servers. (see Wood paragraph [0044], lines 8-14; paragraph [0051], lines 1-3: session token with redirection request)

In addition, the Wood prior art also discloses other redirection methods for the transmission of a session token between servers without storage of the session token at browser. (see Woods paragraph [0050], lines 12-17; paragraph [0051], lines 13-16)

3.2 Applicant argues that the referenced prior art does not disclose, "decrypted session token". (see Remarks Page 12,)

There is no disclosure for the multiple references to the "decrypted" session token in the amended claims. The specification indicates that the second server may not be able to decrypt the session token, therefore the session ID and timestamp are transferred directly to the second server. There is no disclosure of a decrypted session token being processed. (see 112 rejection)

3.3 Applicant argues the dependent claims. (see Remarks Pages 13, 15)

Arguments for dependent claims are based upon above arguments for independent claims 1, 23. The successful responses to arguments for independent claims 1, 23, also successfully respond to the current arguments against the dependent claims 2-6, 9-12 and 24-28, 31-34.

3.4 The Williams prior art discloses a database for the storage of session management information. (see Williams paragraph [0037], lines 10-12; paragraph [0075], lines 12-16: database, storage). In addition, the Williams prior art discloses the capability to redirect service requests from one server to another server. A service request is redirected to a second server for service completion. (see Williams paragraph [0067], lines 12-18: redirection of session token and session information, redirection request for resources)

The Williams prior art discloses a system for secure session management within a collection of web server systems (web farm) using a session token. The claim

limitations disclose that the token is renewed after each use. (see Specification Page 2, Paragraph [0006], lines 7-9) A session management web service updates the session token with each received request. (see Williams paragraph [0016], lines 7-13; paragraph [0016], lines 4-7: generate new encrypted session token and transfer) In addition, the Williams prior art discloses the capability to encrypt and decrypt the session token.

The Williams and Woods prior art combination disclose that if the request must be redirected to a different server where the requested resource is located (see Williams paragraph [0067], lines 12-18: redirection of session token and session information, redirection request for resources) then the decrypted session token is transmitted to the new server (see Wood paragraph [0044], lines 8-14; paragraph [0051], lines 1-3: session token with redirection request) and the session management web service generates a new session token to be used in place of the previous session token. The new session token is transmitted with the requested web resource.

The Williams prior art discloses server(s) utilized for authentication and session token(s) generation. The Williams prior art discloses the capability for session tokens to be encrypted and decrypted during session token processing. (see Williams paragraph [0051], lines 14-16: encryption/decryption utilized for security) Once client access procedures are completed, the Williams prior art processes service requests to access a required resource.

3.5 The examiner has considered the applicant's remarks concerning a system and

method for secure session management in a web farm utilizing a session token, which is updated with each request received from a browser. The capability exists for the redirection of a request to a new server to locate the requested resource, and encryption/decryption of session token(s).

After an additional analysis of the applicant's invention, remarks, and a search of the available prior art, it was determined that the current set of prior art consisting of Williams (20030005118), Wood (20040210771) and Bachman (5,907,621) discloses applicant's invention.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims **1, 13, 23** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

There is no disclosure for the limitation of transmitting said session token directly to the second server. Applicant indicated that paragraph [0038] provides disclosure for this claim limitation. Paragraph [0038] discloses that the extracted session ID and timestamp and not the session token itself are transmitted directly to the server. The

disclosure indicates that this procedure is to avoid the situation where the server cannot decrypt the session token. Paragraph [0023] discloses that the session token includes the session ID and timestamp but it does not disclose that these two parameters are the only parameters in the session token. There is no disclosure within paragraph [0038] for the direct transmission of a session token between two servers.

There is no disclosure within paragraph [0038] for the transmission of a session token directly between two servers. Paragraph [0038] discloses the transmission of the session ID and timestamp and not the session token itself.

There is no disclosure for the multiple references to the "decrypted" session token in the amended claims. The specification indicates that the second server may not be able to decrypt the session token. Therefore the session ID and timestamp are transferred directly to the second server. There is no disclosure of a decrypted session token in the specification or original claims.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims **1 - 6, 9 - 18, 21 - 28, 31 - 34** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Williams et al.** (US PGPUB No. **20030005118**) in view of

Wood et al. (US PGPUB No. **20040210771**).

With Regards to Claims 1, 23, Williams discloses a method, computer program product of secure session management for a web farm, the web farm including a first server and a second server, the second server having a requested web page, the method comprising:

a) receiving, at the first server, a request for the requested web page from a browser, said request including an encrypted session token; (see Williams paragraph [0019], lines 1-5: request processing; paragraph [0016], lines 1-4;: session token; paragraph [0050], lines 10-16; paragraph [0051], lines 14-16: encryption utilized for security; paragraph [0016], lines 1-4: software implementation, program product)

b) decrypting said encrypted session token at the first server to obtain a decrypted session token; (see Williams paragraph [0020], lines 8-11: validate (must decryption required to process encrypted information) session information, process encrypted session information; paragraph [0016], lines 1-4: software implementation, program product)

d) verifying said decrypted session token. (see Williams paragraph [0020], lines 8-11; paragraph [0074], lines 7-11: validate session token information, client and session identification information; paragraph [0016], lines 1-4: software implementation, program product)

Williams discloses wherein redirecting said request to the second server. (see

Williams paragraph [0067], lines 12-18: redirection of session information) Williams does not specifically disclose including transmitting said session token to the second server in a redirect request.

However, Wood discloses:

c) including transmitting said session token directly to the second server; (see Wood paragraph [0044], lines 8-14; paragraph [0051], lines 1-3: session token with redirection request)

It would have been obvious to one of ordinary skill in the art to modify Williams to enable the capability for including transmitting said session token to the second server as taught by Wood. One of ordinary skill in the art would have been motivated to employ the teachings of Wood in order to enable the capability to upgrade session credentials and maintain session continuity. (see Wood paragraph [0016], lines 11-16: "*... The session upgrading means upgrading the session by obtaining and authenticating a second credential to allow access to the target information resource if the first authenticated credential is inconsistent with the trust level requirement. The session upgrade means maintains session continuity across credential upgrades. ...* ")

With Regards to Claims 2, 24, Williams discloses the method, computer program product claimed in claims 1, 23, further including creating a new session token, encrypting said new session token at the second server to produce a new encrypted session token, and transmitting a response to said browser from the second server,

wherein said response includes said new encrypted session token. (see Williams paragraph [0016], lines 7-13; paragraph [0016], lines 4-7: generate new encrypted session token and transfer; paragraph [0016], lines 1-4: software implementation, program product)

With Regards to Claims 3, 5, 15, 17, 25, 27, Williams discloses the method, system, computer program product claimed in claims 2, 13, 14, 23, 24, wherein said decrypted session token includes a session ID and a timestamp, and wherein said creating a new session token includes generating a new session ID and updating said timestamp. (see Williams paragraph [0062], lines 9-16; paragraph [0050], lines 1-5: session token, session ID and timestamp; paragraph [0016], lines 1-4: software implementation, program product)

With Regards to Claims 4, 16, 26, Williams discloses the method, system, computer program product claimed in claims 2, 14, 24, further including a step of updating a common session database by replacing said decrypted session token with said new session token in said common session database. (see Williams paragraph [0069], lines 9-15: database for session token information storage paragraph [0016], lines 1-4: software implementation, program product)

With Regards to Claims 6, 18, 28, Williams discloses the method, system, computer program product claimed in claims 5, 17, 27, wherein a common session database

contains a stored session ID and a stored timestamp, and wherein said verifying includes comparing said session ID and said timestamp with said stored session ID and said stored timestamp. (see Williams paragraph [0069], lines 9-15: database for session token information storage; paragraph [0062], lines 9-16; paragraph [0050], lines 1-5: session token, session ID and timestamp; paragraph [0020], lines 8-11: verification session information paragraph [0016], lines 1-4: software implementation, program product)

With Regards to Claims 9, 21, 31, Williams discloses the method, system, computer program product claimed in claims 1, 13, 23, wherein said step of transmitting includes incorporating said decrypted session token into a URL. (see Williams paragraph [0044], lines 8-12: URL processing techniques utilized paragraph [0016], lines 1-4: software implementation, program product)

With Regards to Claims 10, 32, Williams discloses the method, computer program product claimed in claims 1, 23, wherein a session management web service performs said step of verifying, said session management web service being accessible to said first server and said second server, and wherein said verifying includes comparing said decrypted session token with stored session data. (see Williams paragraph [0020], lines 8-11: session information verification paragraph [0016], lines 1-4: software implementation, program product)

With Regards to Claims 11, 33, Williams discloses the method, computer program product claimed in claims 10, 32, wherein the web farm further includes a common session database containing said stored session data. (see Williams paragraph [0013], lines 5-9; paragraph [0036], lines 3-4: web farms, set of interconnected web servers paragraph [0016], lines 1-4: software implementation, program product)

With Regards to Claims 12, 22, 34, Williams discloses the method, system, computer program product claimed in claims 1, 13, 23, wherein said requested web page includes a web resource selected from the group including an applet, an HTML page, a Java server page, and an Active server page. (see Williams paragraph [0044], lines 3-8; paragraph [0042], lines 8-15: protected resource, a HTML web page paragraph [0016], lines 1-4: software implementation, program product)

With Regards to Claim 13, Williams discloses a system for secure session management, the system being coupled to a network and receiving a request for a requested web page from a browser via the network, the request including an encrypted session token, the system comprising:

a) a first server including a first request handler for receiving the request and decrypting the encrypted session token to produce a decrypted session token; (see Williams paragraph [0013], lines 5-9; paragraph [0050], lines 10-16: multiple servers, encrypted; paragraph [0020], lines 8-11: validate (i.e. must decrypt in order to process) session information)

b) a second server including the requested web page; (see Williams paragraph [0013], lines 5-9: multiple servers; paragraph [0044], lines 3-8; paragraph [0042], lines 8-15: resource requested, a HTML web page)

c) a common session database including stored session data; (see Williams paragraph [0069], lines 9-15: database for session token information storage) and

d) a session management web service, accessible to said first server and said second server and including a validation component for comparing said decrypted session token with said stored session data; (see Williams paragraph [0020], lines 8-11: session verification information)

Williams discloses wherein said first request handler adapted to redirect the request to said second server. (see Williams paragraph [0067], lines 12-18: redirection capabilities) Williams does not specifically disclose whereby transmits the session token to said second server as part of redirected request.

However, Wood discloses:

e) transmit the decrypted session token directly to said second server. (see Wood paragraph [0044], lines 8-14; paragraph [0051], lines 1-3: session token with redirection request)

It would have been obvious to one of ordinary skill in the art to modify Williams to enable the capability for including transmitting said session token to the second server as taught by Wood. One of ordinary skill in the art would have been motivated to employ the teachings of Wood in order to enable the capability to

upgrade session credentials and maintain session continuity. (see Wood paragraph [0016], lines 11-16)

With Regards to Claim 14, Williams discloses the system claimed in claim 13, wherein said session management web service includes a token generator for creating a new session token for said second server, and wherein said second server includes a second request handler, said second request handler encrypting said new session token to produce a new encrypted session token and transmitting a response to said browser, wherein said response includes said new encrypted session token. (see Williams paragraph [0016], lines 7-10; paragraph [0016], lines 4-7: new session token generated and transferred; paragraph [0050], lines 10-16; paragraph [0051], lines 14-16: encrypted session token information)

8. Claims **7, 8, 10, 20, 29, 30** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Williams-Wood** and further in view of **Bachman et al.** (US Patent No. **5,907,621**).

With Regards to Claims 7, 19, 29, Williams discloses the method, system, computer program product claimed in claims 5, 17, 27. (see Williams paragraph [0050], lines 1-5 : time parameter usage and processing; paragraph [0016], lines 1-4: software implementation, program product) Williams does not specifically disclose a time out processing capability. However, Bachman discloses wherein including determining

whether a session has timed out, said step of determining including determining an elapsed time between said timestamp and a current server time, and comparing said elapsed time with a predetermined maximum time to determine whether said session has timed out. (see Bachman col. 1, lines 65-67: session management; col. 4, lines 11-17; col. 6, lines 10-19: process time out condition)

It would have been obvious to one of ordinary skill in the art to modify Williams to enable the capability to process a time period expiration condition as taught by Bachman. One of ordinary skill in the art would have been motivated to employ the teachings of Bachman in order to enable the capability to create a secure communications session between server and client systems and avoid distracting the client with the placement of token information within the page. (see Bachman col. 1, lines 65-67: "*... An advantage of the present invention is that a secure user session can be established between an internet server and a browser at an unsecured client. ...*"; col. 2, lines 15-17: "*... To avoid distracting the user, the token is carried in a field of the page that is normally not displayed in the presentation space. ...*")

With Regards to Claims 8, 20, 30, Williams discloses the method, system, computer program product claimed in claims 7, 19, 29. (see Williams paragraph [0050], lines 1-5: time parameter usage and processing; paragraph [0016], lines 1-4: software implementation, program product) Williams does not specifically disclose a time out processing capability. However Bachman discloses wherein includes closing said session if said session has timed out. (see Bachman col. 1, lines 65-67: session

management; col. 4, lines 11-17; col. 6, lines 10-19: process time out condition, session erased, closed)

It would have been obvious to one of ordinary skill in the art to modify Williams to enable the capability to process a time period expiration condition as taught by Bachman. One of ordinary skill in the art would have been motivated to employ the teachings of Bachman in order to enable the capability to create a secure communications session between server and client systems and avoid distracting the client with the placement of token information within the page. (see Bachman col. 1, lines 65-67; col. 2, lines 15-17)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

CVJ
April 14, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136